

Claims

- 5 1. A method for downloading, updating and/or incrementing applications and/or data from a provider (AP) via a transmission channel of limited bandwidth onto a device (SC), in particular a portable device with limited processing power and/or memory,
characterized by
- 10 - at the provider (AP), generating code blocks Bi of the application or data to be transmitted,
- defining an authentication function comprising a one-way function,
- computing an authentication value $H(Bi)$ for each block Bi to be transmitted,
- selecting an authentication tree for said authentication values $H(Bi)$,
- 15 - computing authentication values Hi of the branches and the root authentication value HT of said tree,
- signing said root authentication value HT , thereby generating $Sign(HT)$,
- generating messages Mi comprising said blocks Bi and, partly, selected ones of said authentication values $H(Bi)$,
- 20 - transmitting said signed root authentication value $Sign(HT)$ and said messages Mi from said provider (AP) to said device (SC),
- in said device (SC), upon receiving any one of said messages Mi , extracting said block Bi , computing the corresponding authentication value $H(Bi)$ and cashing it, computing selected intermediate authentication values Hi along said tree
- 25 until a previously verified authentication value << *has this value a name??* >> is reached,
- comparing said computed intermediate authentication value Hi with said previously verified authentication value and,
- if the values are equal, accepting said received block Bi or, if otherwise, indicating an error.
- 30

009222T 9448446 122500

2. The method according to claim 1, wherein

- the generated code blocks ***Bi*** of the application or data to be transmitted are sequentially transmitted,
- the computing and comparing in the device (SC) is sequentially executed until all blocks ***Bi*** are verified, and
- the application or data is considered correctly received, when no error was indicated.

3. The method according to claim 1 or 2, wherein

- the one-way function of the authentication function is a hashing function,
- the authentication tree is a hash tree ***HT***, in particular a binary and/or symmetrical tree, of the code blocks ***Bi*** generated in the provider (AP).

4. The method according to any of the preceding claims, wherein

- a **SendBlocks** process is defined in the provider (AP), consisting of a several loops which iteratively construct an *i*-th message ***Mi*** consisting either of a block ***Bi*** alone or of a block ***Bi*** plus one or more authentication values ***Hi*** and/or ***H(Bi)***.

5. The method according to claim 4, wherein

- each $2j$ -th message ***Mi*** consists of the corresponding block ***Bi*** alone, whereas each $(2j+1)$ -th message ***Mi*** includes the full or part of the authentication or hash path from the corresponding block ***Bi*** towards the root of the authentication tree.

6. The method according to any of the preceding claims, wherein

- a **ReceiveBlocks** process is defined in the device (SC), consisting of several loops,
- said process iteratively evaluating an *i*-th message ***Mi*** by extracting from a received messages ***Mi*** the corresponding block ***Bi*** and,

- if the received message M_i includes one or more authentication values H_i and/or $H(B_i)$, extracting these values and caching them for later verification.

7. The method according to claim 6, wherein

- storing in the device (SC) only those authentication values $H(B_i)$ and/or H_i and/or HT needed to authenticate subsequently transmitted blocks B_i and
- clearing all authentication values $H(B_i)$ and/or H_i not needed in the further process.

8. A method for transmitting applications and/or data from a sender to a receiver, characterized by

- in said sender, partitioning said applications and/or data into blocks,
- defining an authentication function comprising a one-way function,
- computing an authentication value for each of said blocks,
- selecting an authentication tree for said authentication values of said blocks and computing authentication values of the branches and a root authentication value of said tree,
- sequentially sending said blocks with selected ones of said block and/or branch authentication values and/or said root authentication value to said receiver,
- extracting in said receiver said application or data block,
- computing in said receiver those authentication values that are available along the branch towards the root,
- storing in said receiver authentication values needed to authenticate subsequently transmitted data blocks, and
- verifying in said receiver each subsequently received block with computed and/or stored authentication values.

9. Provider apparatus (AP) for downloading, updating and/or incrementing applications and/or data partitioned into blocks onto a device (SC), in particular a portable device with limited processing power and/or memory, in which apparatus

- an authentication function comprising a one-way function is defined and

- an authentication tree is selected for authenticating said blocks, said apparatus including
 - means (3) for computing an authentication value for each of said blocks and of the branches of said tree,
 - 5 - means (4) for computing a root authentication value,
 - means (5) for building messages from said blocks and selected ones of said authentication values, and
 - transport means (11) for sequentially sending said messages to said receiver.
- 10 10. Device (SC), in particular a portable device with limited processing power and/or memory, for evaluating messages received from a provider (AP) for downloading, updating and/or incrementing applications and/or data partitioned into blocks on said device, in which the provider has
- defined an authentication function comprising a one-way function and
 - 15 - selected an authentication tree is for authenticating said blocks, said device including
 - transport means (11) connected to said provider (AP) for receiving messages from said provider,
 - means (15) for extracting said application or data block and for computing and
 - 20 storing authentication values are available along the branches towards the root of said authentication tree,
 - means (14) for verifying signatures extracted from said blocks and for verifying each subsequently received block with computed and/or stored authentication values, and
 - 25 - storage means (19) for authentication values needed to authenticate subsequently transmitted blocks.

0092227 9448460